सवालीराम

सवालः कम्प्यूटर वायरस किस तरह काम करता है और खुद की प्रतिलिपियाँ बना लेता है?

जवाबः वायरस से लाखों प्रभावित, 10 अरब से ज़्यादा का आर्थिक नुकसान! अगर इस शीर्षक को पढ़कर आप यह सोच रहे हैं कि यहाँ किसी ऐसी जानलेवा बीमारी द्वारा मचाई जा रही तबाही की बात हो रही है जिससे दुनियाभर के लोग प्रभावित हैं, तो यह आपकी गलती नहीं है। यहाँ दरअसल, कम्प्यूटर वायरसों द्वारा व्यापक स्तर पर कम्प्यूटरों को संक्रमित किए जाने की वजह से होने वाले आर्थिक नुकसान की बात हो रही है। कम्प्यूटर वायरसों के द्वारा किए जाने वाले उत्पात और विनाश के वर्णन पढ़ने में इतिहास के विख्यात आक्रमणों और विश्वयुद्धों के वर्णन लग सकते हैं। कम्प्यूटर वायरस व्यक्तियों या कम्पनियों के कम्प्यूटरों को ही नहीं बल्कि पूरी अर्थव्यवस्थाओं को पंगु बना सकते हैं। सारे कम्प्यूटर वायरस मनुष्य द्वारा ही तैयार किए जाते हैं, ऐसे किसी व्यक्ति के द्वारा जिसके पास ऐसा अपराध करने के लिए ज़रूरी बुद्धि, सामर्थ्य और इच्छा हो।

थोड़ा पीछे मुड़कर, पहले ज़रा यह समझते हैं कि कम्प्यूटर वायरस असल में होता क्या है। संक्षेप में कहें, तो यह कम्प्यूटर द्वारा समझी जा सकने वाली



भाषा में तैयार किए गए निर्देशों की कुछ लाइनें (जिन्हें एक कम्प्यूटर प्रोग्राम के रूप में लिखा जाता है) होती हैं। इस तरह के नुकसानदायक प्रोग्राम (मैलिशियस सॉफ्टवेयर या मैलवेयर) के कई अलग-अलग प्रकार होते हैं - वर्म, स्पाईवेयर, ऐडवेयर और ट्रोजन हॉर्स। इनमें से अधिकांश के भीतर यह निर्देश रहते हैं कि उन्हें अपनी प्रतिकृतियाँ कैसे बनाना है, और कम्प्यूटर के अन्य भागों में, या दूसरे कम्प्यूटरों में भी कैसे फैलना है, जो हम आगे देखेंगे।

कम्प्यूटर वायरसों में जैविक संसार के अपने हमनामों की कई विशेषताएँ होती हैं। ये वायरस आपकी अनुमति के बिना आपके कम्प्यूटर के अन्य प्रोग्राम में घुस जाते हैं या कहें कि उन्हें संक्रमित कर देते हैं और फिर जहाँ भी संक्रमित होस्ट (मेज़बान) प्रोग्राम जाते हैं, वहाँ घुस जाते हैं। हर बार जब इन प्रोग्रामों का उपयोग होता है, वायरस भी अपना काम करता है। उदाहरण के लिए, यदि होस्ट प्रोग्राम कोई स्प्रेडशीट या कोई डॉक्यूमेंट है, तो वह जब भी खोला जाएगा, वायरस भी हरकत में आ जाएगा और अपने भीतर निहित निर्देशों का पालन करने लगेगा। इसके अलावा, जैविक विषाणुओं की तरह ही, वायरस प्रोग्राम भी सूक्ष्म होते हैं। यदि वे आकार में बड़े होंगे तो पकड़ में आ सकते हैं।

वायरस किस तरह से खतरनाक होते हैं? आखिर, आपके कम्प्यूटर में घुसकर अपनी प्रतिकृतियाँ बना लेने वाले कुछ लाइनों के ऐसे प्रोग्रामों द्वारा क्या बड़ा नुकसान हो सकता है, खास तौर से अगर वे आकार में काफी छोटे हों और कम्प्यूटर की बहुत ज़्यादा जगह न घेरते हों?

इस खीझ दिलाने वाली बात के अलावा, कि यह एक अनिमंत्रित मेहमान होता है, कम्प्यूटर वायरस में सबसे बड़ी दिक्कत यह है कि इस में पेलोड नामक चीज़ होती है। यही वायरस प्रोग्राम का वह भाग है जो कम्प्यूटर को नुकसान पहुँचा सकता है। ये पेलोड अलग-अलग ढंग से अपना असर दिखा सकते हैं - स्क्रीन पर बेवकूफ और लज्जाजनक सन्देश दिखाने से लेकर महत्वपूर्ण फाइलों को मिटाने तक। पेलोड आपके कम्प्यूटर को बन्द भी कर सकते हैं, वे आपकी हार्ड-ड्राइव को निष्क्रिय कर देते हैं। वे आपकी ज़रूरी और उपयोगी फाइलों को क्षति पहुँचा सकते हैं (करप्ट कर सकते हैं) और उनको पूरी तरह मिटा भी सकते हैं। ये कम्प्यूटर की कोई दैहिक (हार्डवेयर की) क्षति नहीं है, इससे आपके कम्प्यूटर में डले सॉफ्टवेयर को क्षति पहुँचती है। ये फाइलें अन्य प्रोग्राम भी हो सकते हैं या फिर ऐसी फाइलें जिनमें आपका डाटा होता है। ऐसे नुकसान से उबरना मुश्किल हो सकता है। कम्प्यूटर प्रोग्राम यानी सॉफ्टवेयर अकसर काफी महँगे होते हैं। यदि डाटा नष्ट हो गया हो, तो इसका यह मतलब भी हो सकता

है कि वह सारी जानकारी फिर से एकत्रित करके संकलित करनी पड़ेगी। कभी-कभी ऐसा करना असम्भव होता है। इस तरह, आर्थिक नुकसान तो बहुत होता ही है, लेकिन आपकी ज़रूरी जानकारियों के खो जाने का तो हिसाब ही नहीं लगाया जा सकता। पेलोड को कम्प्यूटर के अन्य नियमित कार्यों के माध्यम से भी सक्रिय किया जा सकता है, जैसे आपकी कम्प्यूटर घड़ी के किसी खास समय पर, कीबोर्ड पर किन्हीं खास कुँजियों को हर बार दबाने पर इत्यादि।

वायरस कैसे फैलते हैं?

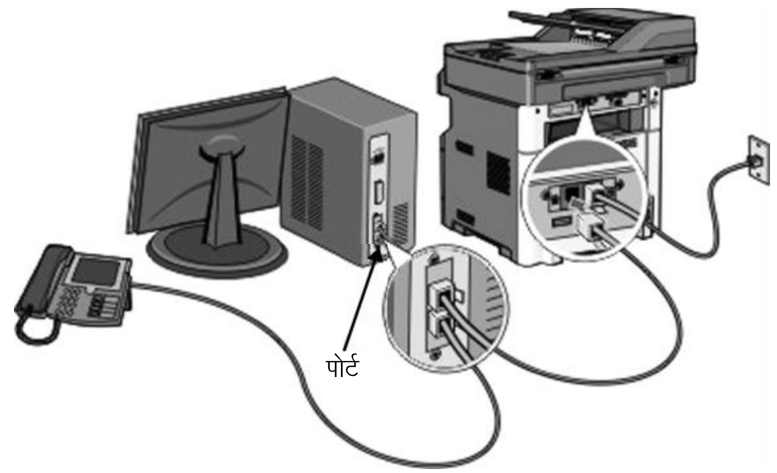
तो वायरस आपके कम्प्यूटर में घुसते कैसे हैं, और किस विधि से फैलते हैं? इंटरनेट के आने से पहले वायरस फ्लॉपी डिस्क जैसी 'रिमूवेबल मेमोरी डिवाइसिज़' (जो कम्प्यूटर में स्थायी न होकर एक से निकाल कर दूसरे कम्प्यूटर में उपयोग किया जा सकता हो) के माध्यम से फैला करते थे। आज, इनकी जगह पेन-ड्राइव या मेमोरी स्टिक ने ले ली है। कोई पेन-ड्राइव वायरस वाले कम्प्यूटर में इस्तेमाल किए जाने पर संक्रमित हो सकती है और फिर जब भी इस पेन-ड्राइव को असंक्रमित कम्प्यूटरों में इस्तेमाल किया जाता है तो यह उनमें भी वायरस फैला देती है।

आजकल कम्प्यूटर वायरस सबसे ज़्यादा इंटरनेट के माध्यम से फैलते हैं। ई-मेल के माध्यम से यह हो सकता है। आप में से ई-मेल का उपयोग करने वाले लोगों को अकसर ऐसे ई-मेल आते होंगे जिनमें फाइलें संलग्न रहती हैं। ये फाइलें कभी-कभी वायरस होती हैं और वे कोई ऐसा आकर्षक छद्म रूप भी धर सकती हैं जिससे आपकी जिज्ञासा जाग जाए। उदाहरण के लिए, आपको ऐसा ई-मेल मिल सकता है जिसमें कहा गया हो कि





मेमोरी डिवाइसिज़: कम्प्यूटर में आसानी से लगाई जाने वाली मेमोरी युक्तियाँ जैसे फ्लॉपी डिस्क, पेन-ड्राइव, मेमोरी कार्ड आदि।



कम्प्यूटर के पोर्ट: एक कम्प्यूटर आम तौर पर केबल/तारों के ज़रिए फोन लाइन, प्रिंटर आदि से जुड़े रहते हैं। आजकल बिना तारों के, वायरलेस कनेक्शन सामान्य हैं। ऐसे ही कम्प्यूटर भी एक-दूसरे के सम्पर्क में रहते हैं।

यदि आप संलग्न फाइल को खोलते हैं तो आप एक उपहार हासिल करने के पात्र होंगे। जिज्ञासावश, उत्सुकता के चलते आप उसे खोल देते हैं। ये कोई कम्प्यूटर वायरस हो सकता है जो उस फाइल को खोलने के साथ ही आपके ई-मेल अकाउंट से आपके कम्प्यूटर में डाउनलोड हो जाता है। इसके बाद उस वायरस का पेलोड आपके कम्प्यूटर में अपना हानिकारक काम शुरू कर देता है। इस वायरस के अन्दर आपके ई-मेल अकाउंट में मौजूद सभी पतों पर अपनी प्रतिकृति युक्त ई-मेल भेजने के निर्देश भी हो सकते हैं। आपके परिचितों को आपके नाम से ई-मेल मिलेगा जो दरअसल, आपने नहीं भेजा है। और यदि वे अटैचमेंट (संलग्न फाइल) को खोलते हैं, तो यही प्रक्रिया उनके साथ भी दोहराई जाएगी। किसी वेबसाइट पर जाने के सामान्य से कृत्य के द्वारा भी वायरस डाउनलोड हो सकता है।

इसके अलावा कम्प्यूटर पोर्ट के माध्यम से भी इंटरनेट, और अन्य नेटवर्क (उन कम्प्यूटरों के संजाल जो एक-दूसरे के साथ इन्टरनेट के माध्यम से नहीं बल्कि तारों के माध्यम से जुड़े होते हैं) का उपयोग वायरसों को फैलाने के लिए किया जा सकता है। हर कम्प्यूटर में ऐसे स्लॉट (खाँचे) बने होते हैं जिन्हें पोर्ट कहा जाता है। ये वे स्थान होते हैं जहाँ आपके कम्प्यूटर से जुड़ने वाले मोडेम, प्रिंटर और अन्य मशीनों के तारों को जोड़ा जाता है।

यदि आपका कम्प्यूटर चालू है और इन नेटवर्कों से जुड़ा हुआ है, तो इन दूसरी मशीनों में मौजूद मैलवेयर उसमें भी दाखिल हो सकते हैं।

वायरस के विभिन्न रूप

अकसर, वायरस आपके कम्प्यूटर को कोई क्षति नहीं पहुँचाते। उनके अपने और ज़्यादा कुटिल उद्देश्य होते हैं। कुछ वायरस ऐसे होते हैं जिन्हें आपसे जुड़ी जानकारियों को एकत्रित करने के लिए तैयार किया जाता है। ये आपकी जासूसी करते हैं, इन्हें स्पाईवेयर कहा जाता है। ये आपके पासवर्ड का, और ऑनलाइन खरीदारियों के दौरान होने वाले आर्थिक लेन-देन से आपके क्रेडिट या डेबिट कार्ड की जानकारियों तक का संग्रह कर लेते हैं। ये प्रोग्राम आपके द्वारा अपने कम्प्यूटर पर की जाने वाली हर गतिविधि को, यानी कीबोर्ड पर दबाई जाने वाली हर एक कुँजी को दर्ज़ करके उसकी जानकारी अपने बनाने वाले तक पहुँचा देते हैं।

ऐसे वायरसों का एक सम्भावित हानिरहित रूप होता है ऐडवेयर। ऐडवेयर ऐसे प्रोग्राम होते हैं जो खुद आपके कम्प्यूटर में इंस्टॉल हो जाते हैं, आप जिन वेबसाइटों पर जाते हैं, उन पर नज़र रखते हैं और आपकी स्क्रीन पर विज्ञापन दिखाने लगते हैं। आप इस बात से अनभिज्ञ हो सकते हैं कि ये विज्ञापन आपके कम्प्यूटर से ही आ रहे हैं, न कि आपके द्वारा विज़िट की जाने वाली साइटों से।

कुछ वायरसों की दिलचस्पी आपको नुकसान पहुँचाने में उतनी नहीं होती जितनी आपका इस्तेमाल करने में होती है। आपके कम्प्यूटर में कुछ ऐसी चीज़ हो सकती है जो वायरस के लेखक के लिए मूल्यवान हो - जगह, या मेमोरी। कुछ लोग ऐसे प्रोग्राम तैयार करते हैं कि वे आपके कम्प्यूटर में प्रवेश कर सकें या उसे 'हैक' कर सकें ताकि वे इसका उपयोग, या तो बहुत बड़ी संख्या में ई-मेल भेजने के लिए कर सकें, या फिर कोई ऐसा प्रोग्राम चलाने के लिए कर सकें जिसे बहुत अधिक मेमोरी की ज़रूरत पड़ती हो। आम तौर पर, ऐसी योजनाओं के द्वारा वे लोग (हैकर्स) पैसा बनाते हैं।

वायरस से बचना

वायरसों से अपने कम्प्यूटर की सुरक्षा करने का सबसे अच्छा तरीका है ऐंटी-वायरस सॉफ्टवेयर या फायरवॉल जैसे प्रोग्राम का उपयोग करना। किसी भी अनुचित प्रवेश के विरुद्ध आपके कम्प्यूटर की पहली सुरक्षा पंक्ति होती है फायरवॉल जो वायरसों को आपके कम्प्यूटर के प्रवेशद्वारों, यानी उसके पोर्ट पर पहुँचते ही पकड़ लेता है। ऐंटी-वायरस सॉफ्टवेयर उन वायरसों को पकड़ते हैं जिन्होंने इस सुरक्षा-दीवार को भेद दिया हो, और सम्भवतः आपके कम्प्यूटर में मौजूद फाइलों तक पहुँच गए हों।

हर महीने सैकड़ों नए वायरस बनाए जाते हैं, इसलिए अपने कम्प्यूटर को वायरसों से बचाना अच्छी-खासी चुनौती हो सकती है। एहतियाती उपायों - जैसे ई-मेल के साथ संलग्न फाइलों, अटैचमेंट को तभी खोलना जब आप सुनिश्चित हों कि वे ई-मेल भरोसेमन्द स्रोतों से आए हैं और वे कोई नकली सन्देश नहीं हैं - के अलावा आपको यह सुनिश्चित करना भी ज़रूरी है कि अपने कम्प्यूटर से आप जिस भी डिस्क या ड्राइव या मशीन को जोड़ रहे हों, वह वायरस-मुक्त हो। इन तमाम एहतियातों के बावजूद, नए वायरस आपके कम्प्यूटर में दाखिल हो सकते हैं, और उनसे निपटने का एक ही तरीका है कि आप अपने ऐंटी-वायरस सॉफ्टवेयर को निरन्तर अपडेट करते रहें।

कम्प्यूटर वायरसों को पकड़ पाना मुश्किल हो सकता है, हालाँकि इनके कुछ संकेत हो सकते हैं जैसे आपके प्रोग्रामों को लोड होने में देर लग रही हो, आपके कम्प्यूटर में आपके अनुमान से कम जगह रह जाए, आपके फोल्डरों में नई या विचित्र-से नामों वाली फाइलें दिखाई दें, या आपकी ड्राइव की बत्ती टिमटिमाती रहे भले ही आप उस पर कोई काम न कर रहे हों इत्यादि। ऐसे में आपके लिए सबसे बढ़िया उपाय होगा अपडेट किया हुआ ऐंटी-वायरस सॉफ्टवेयर इस्तेमाल करना और उसके द्वारा समस्याओं की जाँच करना। आम तौर पर इन सॉफ्टवेयर को बनाने वाली कम्पनियाँ नए आने वाले वायरसों से सिर्फ कुछ ही दिन पीछे चलती हैं।

कुछ इतिहास कुछ उदाहरण

कम्प्यूटर वायरस लगभग उतने ही पुराने हैं जितने कि कम्प्यूटर। प्रारम्भिक कम्प्यूटरों के बनने के करीब एक दशक बाद, 1940 के दशक के अन्तिम वर्षों में पहला वायरस विकसित किया गया। उस समय उन्हें 'वायरस' नाम से नहीं जाना जाता था। कम्प्यूटर विज्ञान के कुछ क्षेत्रों (जैसे रोबोटिक्स) में ऐसे प्रोग्रामों की ज़रूरत पड़ी जो खुद-ब-खुद अपनी प्रतिकृतियाँ बना सकते थे। जिस रूप में आज हम उन्हें जानते हैं, उस तरह का पहला कम्प्यूटर वायरस 1982 में एक पन्द्रह वर्षीय विद्यार्थी द्वारा बतौर मज़ाक बनाया गया था। इसके काफी समय बाद तक यह स्थिति रही कि वायरसों को फैलने के लिए मनुष्यों की ज़रूरत होती थी। कोई भी वायरस तभी एक कम्प्यूटर से दूसरे कम्प्यूटर में पहुँच सकता था जब उसे किसी डिस्क में कॉपी करके उस डिस्क को दूसरे कम्प्यूटर में इस्तेमाल किया जाता। उस समय, कम्प्यूटर मुख्य रूप से एकल रूप में ही चलाए जाते थे। वे विस्तृत नेटवर्क (एक-दूसरे से जुड़े कम्प्यूटरों का समूह, जिसमें आप तारों के माध्यम से जुड़े उस नेटवर्क के अन्य कम्प्यूटरों की फाइलों तक पहुँच सकते हैं) में कम पाए जाते थे। इन्टरनेट के आने के साथ, इन वायरसों को एक कम्प्यूटर से दूसरे कम्प्यूटर तक जाने के लिए

सिर्फ एक मोडेम कनेक्शन की ज़रूरत रह गई।

एक प्रारम्भिक कम्प्यूटर वायरस पाकिस्तान में कम्प्यूटर स्टोर चलाने वाले दो भाइयों द्वारा बनाया गया था जो प्रोग्रामर्स भी थे। उनका ध्यान अपनी एक फ्लॉपी डिस्क पर गया जिस पर कम्प्यूटर के चालू होते ही किसी प्रोग्राम को चलाने के निर्देश थे। उन्होंने इन निर्देशों से कुछ ऐसी छेड़छाड़ की, कि उस डिस्क का लेबल (डिस्क का एक हिस्सा जिसमें ज़रूरी जानकारी रहती है) बदलकर 'ब्रेन' बना दिया गया। उन्होंने इसमें ऐसे निर्देश भी डाल दिए कि उस ड्राइव में आइन्दा डाली जाने वाली सभी फ्लॉपी डिस्कों पर भी वे निर्देश कॉपी हो जाएँ। यह बात है 1980 के दशक के मध्य की। अगले कुछ सालों में यह वायरस दुनियाभर में फैल गया, और अमरीका तक के कम्प्यूटरों में पाया गया। हालाँकि, यह अपेक्षाकृत हानिरहित वायरस था। कुछ इतने हानिरहित नहीं थे, पर मज़ेदार थे। जैसे कि कैसकेड वायरस - इसमें स्क्रीन पर दिखाई देने वाले सभी अक्षर और संख्याएँ एक बड़े ढ़ेर के रूप में स्क्रीन के तल पर गिरती चली जाती थीं। या फिर 'जोशी वायरस', जिसे मुम्बई के एक कम्प्यूटर इंजिनियर ने 1990 में तैयार किया। संक्रमित कम्प्यूटर में जनवरी 5 को यह वायरस सक्रिय हो जाते हैं - स्क्रीन हरा रंग का हो जाता है और 'टाइप - हैप्पी बर्थडे जोशी!' अँग्रेज़ी में प्रकट होता है। और जब तक आप ऐसा टाइप नहीं करते, आपकी मशीन आगे नहीं बढ़ेगी।



डेविड एल स्मिथः मेलिसा वायरस के रचयिता। जिनको अमरीका अदालत ने कारावास और 5,000 डॉलर जुर्माना की सज़ा सुनाई। साथ ही उन्हें अन्य वायरस रचयिताओं को पकड़वाने में पुलिस की मदद करनी पड़ी।

हालाँकि, इसके बाद जल्दी ही मैलीशियस पेलोड वायरसों के साथ जोड़े जाने लगे। साथ ही, ऑपरेटिंग सिस्टम के रूप में डॉस का स्थान विंडोज़ ने ले लिया, जिस पर वायरसों का प्रभाव ज़्यादा आसानी से हो जाता है। इस पर चर्चा किसी और दिन

करेंगे। उदाहरण के लिए, पिछले कुछ सालों के सबसे घातक वायरसों में से एक था 'मेलिसा वायरस' - जिसने मार्च 1999 में कॉरपोरेट नेटवर्कों में ई-मेल सन्देशों की बाढ़ ला दी। माइक्रोसॉफ्ट आउटलुक (ई-मेल को डाउनलोड करके व्यवस्थित करने वाला एक प्रोग्राम) के माध्यम से जैसे ही व्यक्ति संक्रमित अटैचमेंट वाले ई-मेल सन्देश को खोलता था, उसकी ऐड्रेस बुक के पहले 50 नामों को वायरस भेज दिया जाता था। इस ई-मेल को प्राप्त करने वाले कई लोगों ने धोखा खाया क्योंकि भेजने वालों के नामों से ये लोग परिचित थे और इनमें किसी ऐसे डॉक्यूमेंट का हवाला दिया होता था जिसकी कथित माँग प्राप्तकर्ताओं द्वारा की गई थी। इस वायरस ने बहुत कम समय में इतना अधिक ई-मेल ट्रैफिक पैदा कर दिया था कि इंटेल और माइक्रोसॉफ्ट जैसी कम्पनियों को अपने ई-मेल सर्वर बन्द करने पड़े थे। 'मेलिसा वायरस' ऐसा पहला वायरस था जो अपने आप से एक कम्प्यूटर मशीन से दूसरी में पहुँचने में समर्थ था।

कम्प्यूटर वायरस कहीं नहीं जाने वाले। जिस तरह शिकारियों से बचने के लिए शिकार तेज़ी से भागता है, और फिर उसे पकड़ने के लिए शिकारी और तेज़ भागता है, ठीक उसी तरह वायरस और उन्हें पकड़ने के लिए किए जाने वाले उपायों के बीच भी एक तरह की दौड़ मची रहती है। जिस तरह इन वायरसों को बनाने वाले नए-नए प्रयास कर रहे हैं, ऐंटी-वायरस सॉफ्टवेयर निर्माताओं के लिए भी उनकी बराबरी से, बल्कि उनसे एक कदम आगे जाकर काम करना ज़रूरी हो गया है। वायरसों से बचने का कोई एकदम पक्का और विश्वसनीय तरीका नहीं है, लेकिन उनके बारे में जानकर हम अपने कम्प्यूटरों की बेहतर ढंग से रक्षा कर पाएँगे।

इस जवाब को विनता विश्वनाथन ने तैयार किया है।

अँग्रेज़ी से अनुवादः भरत त्रिपाठीः पत्रकारिता का अध्ययन। स्वतंत्र लेखन और द्विभाषिक अनुवाद करते हैं। होशंगाबाद में निवास।

■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

सवालीराम

इस बार का सवालः

क्या बादल का वज़न पता किया जा सकता है?

आप इस सवाल का जवाब 'संदर्भ' को डाक या ई-मेल से भेज सकते हैं।